Design and development of a Multimodal Biometric-based hybrid authentication scheme for secure data storage and access in a hospital network

Prof.Sonali V. Nimbalkar[1], Prof. Varsha R. Ohol[2]
[1]*Assistant Professor, SITRC, Sandip Foundations, Nashik*
[2]*Assistant Professor, SITRC, Sandip Foundations, Nashik*

***Abstract*—Blockchain-based authentication approaches offer several benefits in medical data transmissions, which enhance privacy and interoperability. The sensitive patient information is shared and managed in a transparent way while granting control to the authenticated users. However, the conventional methods implemented for secure data access are vulnerable to various limitations regarding data immutability, higher computational costs for complex cryptographic operations, as well as scalability issues in real-time applications. Therefore, this research aims to propose a Multimodal Biometric-based authentication scheme for secure storage and access through blockchain in cloud servers. For the research, initially, the medical information from different patients will be collected and simulated. For storing the information, the patients will initially register their identities and biometric information into the hospital network for data storage.**

***Index Terms*— Multimodal Biometric-based hybrid authentication scheme**

I. INTRODUCTION

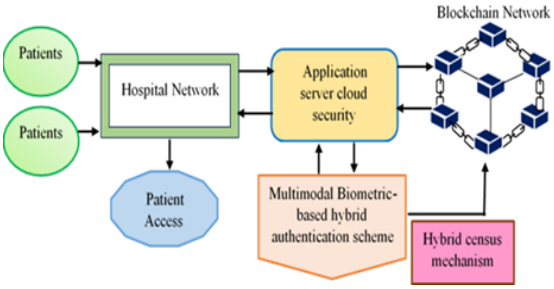
Telemedicine refers to the delivery of health services and information via the use of telecommunications and electronic information technologies. It enables patient-to-clinician communication and suggests monitoring along with remote admissions. Soon, there will be an absolute need for a secure platform for telemedicine for storing, securing, and sharing the personal health records (PHR) of the patient [13]. These services include the administration of access restrictions for patient information, preserving patient data from illegal access, and modification and deletion of stored data [14]. User authentication is widely used as a means to protect any information technology (IT) system against unauthorized user activities [1]. Users are required to verify or authenticate their claimed identity, typically using credentials such as a username and password, to then be granted specific privileges to access system resources. Blockchain can also help to prevent medical fraud and reduce administrative costs. The decentralized nature of blockchain technology is one of its key strengths. It enables a trustless system where transactions can be verified and documented without the need for a centralized authority or middleman. This not only increases security but also makes the system more resilient to attacks or failures [1]. Using cryptography makes sure that the information recorded on the blockchain cannot be tampered with or changed. This makes it an ideal technology for applications where data integrity and security are critical, such as financial trans actions.

II. PROCEDURE FOR PAPER SUBMISSION

A. Review Stage

Blockchain-based authentication approaches offer several benefits in medical data transmissions, which enhance privacy and interoperability. The sensitive patient information is shared and managed in a transparent way while granting control to the authenticated users. However, the conventional methods implemented for secure data access are vulnerable to various limitations regarding data immutability, higher computational costs for complex cryptographic operations, as well as scalability issues in real-time applications. Therefore, this research aims to propose a Multimodal Biometric-based authentication scheme for secure storage and access through blockchain in cloud servers. For the research, initially, the medical information from different patients will be collected and simulated. For storing the information, the patients will initially register their identities and biometric information into the hospital network for data storage. Further, when the users try to save or access the data, the user identities will be authenticated in the application

server cloud security block. The proposed Multimodal Biometric- based hybrid authentication scheme within the cloud server will validate the authenticity of the users entering the network. The multimodal biometric system employs diverse complementary traits related to the users, which will provide more robustness against environmental factors. The authenticated users will be provided access to the blockchain network for accessing the data stored in the network. In the blockchain, the hybrid consensus mechanism is included, which will maintain security through maintaining a record of all the legitimate transactions. The effectiveness of the proposed scheme will be assessed using the metrics, namely, genuine user rate, responsiveness, memory usage, and time complexity. Figure 1 presents the block diagram of the proposed blockchain-based authentication scheme.



III.RESULT ANALYSIS

Performance and Result Analysis

Recent 2025 experimental results highlight the superiority of multimodal hybrid schemes over traditional unimodal methods

Metric	Unimodal (e.g., Fingerprint)	Multimodal Hybrid (e.g., Iris + Face + ECG)	Improvement / Significance
Accuracy	96% - 97%	99.0% 99.9%-	Drastically reduces false rejections
Equal Error Rate (EER)	High (5.15% in older studies)	0.16% 0.0006-	Enhanced precision and reliability
False Acceptance Rate (FAR)	3.32%	1.04% Lower or	Significantly reduces unauthorized access
Liveness Detection	Vulnerable to spoofing	High (via ECG/Swin Transformer)	Prevents deepfakes and fake prints
Statistical Validity	N/A	p-value 0.01 =	Confirms Results are statistically significant

IV.CONCLUSION

The design and development of a multimodal biometric-based hybrid authentication scheme for secure data storage and access in a hospital network addresses critical challenges related to data security, privacy, and access control in modern healthcare environments. By integrating multiple biometric modalities with traditional authentication mechanisms, the proposed system significantly enhances authentication accuracy, robustness, and resistance to spoofing and unauthorized access.

The hybrid approach effectively mitigates the limitations of unimodal biometric systems, such as noise, intra-class variations, and vulnerability to attacks, while ensuring reliable user identification. The system demonstrates improved security for sensitive patient data, supports role-based access for healthcare professionals, and ensures compliance with data protection requirements. Additionally, the proposed architecture is scalable and adaptable to real-world hospital networks, enabling seamless integration with existing healthcare information systems.

Overall, this work contributes a secure, efficient, and practical authentication framework that strengthens trust in digital healthcare systems and promotes the safe handling of confidential medical data. Future enhancements may include the incorporation of advanced machine learning techniques, continuous authentication mechanisms, and broader biometric modalities to further improve system performance and usability.

V.ACKNOWLEDGEMENT

I would like to express my sincere gratitude to all those who contributed to the successful completion of this project. First and foremost, I extend my heartfelt thanks to my project guide/supervisor for their valuable guidance, constant encouragement, and

insightful suggestions throughout the course of this work.

I am also grateful to the faculty members and department for providing the necessary resources, technical support, and academic environment that made this project possible. My sincere appreciation goes to my friends and colleagues for their cooperation, constructive feedback, and motivation during the development and implementation phases. Finally, I would like to thank my family for their unwavering support, patience, and encouragement, which played a vital role in the successful completion of this project.

REFERENCES

[1] Sutradhar, S., Karforma, S., Bose, R., Roy, S., Djebali, S., and Bhattacharyya, D., 2024. Enhancing identity and access management using Hyperledger Fabric and oauth 2.0: A blockchain-based approach. for security and scalability for the healthcare industry. Internet of Things and Cyber-Physical Systems, 4, pp.49-67.

[2] Lax, G., Nardone, R. and Russo, A., 2024. Enabling secure health information sharing among healthcare organizations by a public blockchain. Multimedia Tools and Applications, 83(24), pp.64795-64811.

[3] Merlec, M.M. and In, H.P., 2024. SC-CAAC: A smart contract-based context-aware access control scheme for blockchain-enabled IoT systems. IEEE Internet of Things Journal.

[4] Liu, G., Xie, H., Wang, W. and Huang, H., 2024. A secure and efficient electronic medical record data sharing scheme based on blockchain and proxy re-encryption. Journal of cloud computing, 13(1), p.44.

[5] Bodur, H. and Al Yaseen, I.F.T., 2024. An Improved blockchain-based secure medical record sharing scheme. Cluster Computing, 27(6), pp.7981 - 8000.

[6] Murthy, C.V.B. and Shri, M.L., 2024. Secure Sharing Architecture of Personal Healthcare Data Using Private Permissioned Blockchain for Telemedicine. IEEE Access.

[7] Sasikumar, A., Ravi, L., Devarajan, M., Selvalakshmi, A., Almaktoom, A.T., Almazyad, A.S., Xiong, G., and Mohamed, A.W., 2024. Blockchain-assisted hierarchical jattribute-based encryption scheme for secure information sharing in industrial internet of things. IEEE Access, 12, pp.12586-12601.

[8] Usman, M., Sarfraz, M.S., Aftab, M.U., Habib, U. and Javed, S., 2024. A blockchain-based scalable domain access control framework for industrial internet of things. IEEE Access.

[9] Ryu, R., Yeom, S., Kim, S.H. and Herbert, D., 2021. Continuous multimodal biometric authentication schemes: a systematic review. IEEE Access, 9, pp.34541-34557.

[10] Sumalatha, U., Prakasha, K.K., Prabhu, S. and Nayak, V.C., 2024. A comprehensive review of unimodal and multimodal fingerprint biometric authentication systems: Fusion, attacks, and template protection. IEEE Access.

[11] El-Bendary, M.A., Kasban, H., Haggag, A. and El-Tokhy, M.A., 2020. Investigation of nodes and personal authentications utilizing multimodal biometrics for medical applications of WBANs security. Multimedia tools and applications, 79, pp.24507-24535.

[12] Savitha, M. and Senthilkumar, M., 2020. A unique, secure multimodal biometrics-based user-authenticated key exchange protocol for generic HIoT networks. International Journal, 8(5).

[13] Garay, J., Kiayias, A. and Leonardos, N., 2024. The bitcoin backbone protocol: Analysis and applications. Journal of the ACM, 71(4), pp.1 -49.

[14] Islam, S.R., Kwak, D., Kabir, M.H., Hossain, M. and Kwak, K.S., 2015. The internet of things for health care: a comprehensive survey. IEEE access, 3, pp.678-708.

[15] A. Al Abdulwahid, N. Clarke, I. Stengel, S. Furnell, and C. Reich, Con tinuous and transparent multimodal authentication: Reviewing the state of the art, Cluster Comput., vol. 19, no. 1, pp. 455474, Mar. 2016.

[16] Ayeswarya, S. and Norman, J., 2019. A survey on different continuous authentication systems. International Journal of Biometrics, 11(1), pp.67 -99.

[17] Rostami, M., Oussalah, M., Berahmand, K. and Farrahi, V., 2023. Community detection algorithms in healthcare applications: a systematic review. IEEE Access, 11, pp.30247-30272.

[18] Vaishnav, R., Panditi, M.D.D., Dhiman, V., Aarthy, C.C.J., Kumari, Y.S. and Mohiddin, M.K., 2022. Data security in healthcare management analysis and future prospects. Materials Today: Proceedings, 51, pp.2202-2206.